THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA

CRYSTAL HERNANDEZ and SALVADOR FLORES HERNANDEZ, on behalf of themselves and all others similarly situated, Plaintiffs, v. ADVANCE AMERICA, CASH ADVANCE CENTERS, INC. and ADVANCE AMERICA, CASH ADVANCE CENTERS OF CALIFORNIA, LLC, Defendants.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Crystal Hernandez and Salvador Flores Hernandez ("Plaintiffs") bring this Class Action Complaint against Advance America, Cash Advance Centers, Inc. ("AA") and Advance America, Cash Advance Centers of California, LLC ("AA of California") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] of more than 80,000 individuals, including, but not limited to, name and Social Security number.

2. Defendants provide consumer financial services, including payday loans,

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

installment loans, title loans, and personal lines of credit.

3. AA has dozens of subsidiaries across numerous states, including AA of California.[2]

4. Defendants' Privacy Policy, posted on their website, states as follows:

> **How does Advance America protect my personal information?**
> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.[3]

5. Defendants' Security Information, posted on their website, states as follows:

> **Security of Your Information with Advance America**
>
> With Advance America, you can be sure that all the information you submit is sent through a secure server, and we keep your information in a secure database.[4]

6. Defendants' website also states "[a]ll of our online loan applications include robust security and encryption to ensure your personal data is as secure as possible."[5]

---

[2] AA's subsidiaries include Advance America, Cash Advance Centers of Alabama, LLC; Advance America, Cash Advance Centers of California, LLC; Advance America, Cash Advance Centers of Colorado, LLC; Advance America, Cash Advance Centers of Florida, LLC; Advance America, Cash Advance Centers of Idaho, Inc.; Advance America, Cash Advance Centers of Illinois, Inc.; Advance America, Cash Advance Centers of Indiana, Inc.; Advance America, Cash Advance Centers of Kansas, Inc.; Advance America, Cash Advance Centers of Kentucky, Inc.; Advance America, Cash Advance Centers of Louisiana, LLC; Advance America, Cash Advance Centers of Mississippi, LLC; Advance America, Cash Advance Centers of Missouri, Inc.; Advance America Small Loans of Ohio, Inc.; Advance America, Cash Advance Centers of Ohio, Inc.; Advance America, Cash Advance Centers of Oklahoma, Inc.; Advance America, Cash Advance Centers of South Carolina, Inc.; Advance America, Cash Advance Centers of Tennessee, Inc.; ACSO of Texas, L.P.; Advance America, Cash Advance Centers of Utah, Inc.; Advance America, Cash Advance Centers of Washington, LLC; Advance America, Cash Advance Centers of Wisconsin, Inc.; Advance America, Cash Advance Centers of Wyoming, Inc.; Advance America, Cash Advance Centers of Nevada, Inc.; Advance America, Cash Advance Centers of Virginia, Inc.

[3] Exhibit 1 (Privacy Policy).

[4] Exhibit 2 (Security Information).

[5] Exhibit 3 (Are Online Payday Loans Safe?)

7. Prior to and through February 7, 2023, Defendants obtained the PII of Plaintiffs and Class Members, including by collecting it directly from Plaintiffs and Class Members.

8. Prior to and through February 7, 2023, Defendants stored the PII of Plaintiffs and Class Members, unencrypted, on their network.

9. On or around February 7, 2023, Defendants learned of a data breach on their corporate network during which an unauthorized actor accessed or acquired certain corporate business records on Defendants' network (the "Data Breach").

10. Defendants determined that, during the Data Breach, an unauthorized actor accessed or acquired the PII of Plaintiffs and Class Members.

11. On or around March 23, 2023, reports began surfacing on the Internet that Defendants had been the subject of a ransomware attack by the "BlackBasta" ransomware family and that information obtained during the attack had surfaced on the dark web, including samples containing Social Security numbers and driver's license numbers.

12. On or around August 16, 2023, Defendants began notifying various states Attorneys General of the Data Breach.

13. On or around August 16, 2023, Defendants began notifying Plaintiffs and Class Members of the Data Breach.

14. The notices that Defendants sent to various states Attorneys General and to Plaintiffs and Class Members did not disclose that (i) Plaintiffs' and Class Members' PII was actually acquired by an unauthorized actor during the Data Breach, (ii) the PII had been made available for sale on the dark web, and (iii) whether the threat actor had demanded a ransom and, if so, whether Defendants has refused to pay it.

15. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs

and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII that was accessed and/or acquired by an unauthorized actor included name and Social Security number.

16. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

17. The PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members, including the failure to encrypt the PII and the failure to ensure that Defendants maintained it in encrypted form.

18. As a result of the Data Breach, Plaintiffs and Class Members are, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

19. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; and (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices. Defendants' conduct amounts to negligence and violates federal and state statutes.

20. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

21. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

22. Plaintiff Crystal Hernandez is a citizen of California residing in Bakersfield, California.

23. Plaintiff Salvador Flores Hernandez is a citizen of California residing in Shafter, California.

24. Defendant AA is a Delaware corporation with a principal place of business in Spartanburg, South Carolina.

25. Defendant AA of California is a Delaware limited liability company with a principal place of business in Spartanburg, South Carolina.

26. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

27. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

28. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendants to establish minimal diversity.

29. Defendant AA is a citizen of Delaware and South Carolina because it is a corporation formed under Delaware law with its principal place of business in Spartanburg, South Carolina.

30. Under 28 U.S.C. § 1332(d)(10), Defendant AA of California is a citizen of Delaware and South Carolina because it is a Delaware limited liability company and its principal place of business is in Spartanburg, South Carolina.

31. The District of South Carolina has personal jurisdiction over Defendants because they conduct substantial business in South Carolina and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

32. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants operate in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendants collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

33. Defendants collected the PII of Plaintiffs and Class Members and stored it in an Internet-accessible environment on their network.

34. Plaintiffs and Class Members relied on this sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

35. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

36. On or about August 16, 2023, Defendants sent Plaintiffs and Class Members a *Notice of Data Breach* and submitted sample notices to various states' Attorneys General. Defendants informed Plaintiffs and other Class Members that:

> <<b2b_text_2 (Entity Name)>> d/b/a Advance America ("the Company" or "we") is writing to inform you of a data security incident that may have impacted some of your personal information. We collected personal information about you when

> you applied to receive a loan or another financial service from us and/or became an active customer. We want to provide you with details about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.
>
> **What Happened**
>
> On or around February 7, 2023, we experienced a temporary systems outage affecting our corporate network. Upon becoming aware of the incident, we immediately launched an investigation to better understand the scope and impact of the incident. We also engaged third-party cybersecurity experts to remediate, further investigate what happened, and determine the scope of the incident. Our investigation determined that an unauthorized actor accessed or acquired certain corporate business records on the Company's network. We also reported this incident to law enforcement.
>
> **What We Discovered**
>
> We conducted a thorough review of these business records to identify the individuals whose information was contained in the records. We recently completed this review and determined that some of your information was included in the records.
>
> **What Information Was Involved**
>
> The impacted personal information relating to you includes your <<b2b_text_1(DataElements)>>.[6]

37. Each Plaintiffs' *Notice of Data Breach* states that their name and Social Security number were impacted in the Data Breach.

38. Defendants admitted in the *Notice of Data Breach* and the sample notices and reports they sent to the states' Attorneys General that an unauthorized actor may have acquired sensitive information about Plaintiffs and Class Members, including name and Social Security number.

39. In response to the Data Breach, Defendants claims that they "implemented

[6] Exhibit 4 (sample Notice of Data Breach filed with California Attorney General).

additional security measures to further fortify their network's security measures and protocols and protect customers' information, including leading industry security tools and improved monitoring, enhancing administrative and technical safeguards, and instituting more frequent and rigorous security training."[7]

40. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

41. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

42. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

43. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack on Defendants' network.

44. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack on Defendants' network.

[7] *Id.*

45. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendants Acquire, Collect, and Store the PII of Plaintiffs and Class Members.

46. Defendants acquired, collected, and stored the PII of Plaintiffs and Class Members.

47. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

48. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

49. Defendants could have prevented this Data Breach by properly encrypting the PII of Plaintiffs and Class Members and ensuring that Defendants maintained it in encrypted form.

50. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

51. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

53. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

54. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

---

[8] 17 C.F.R. § 248.201 (2013).

[9] *Id.*

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 24, 2023).

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 24, 2023).

[12] *In the Dark,* VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 24, 2023

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[13]

57. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

58. The fraudulent activity resulting from the Data Breach may not come to light for years.

59. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future

[13] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 24, 2023).

harm.[14]

60. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur from the breach of Defendants' network, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

61. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

62. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in the PII they stored on their network, amounting to thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

63. To date, Defendants have offered Plaintiffs and Class Members one year of identity monitoring and protection services. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

64. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 24, 2023).

Plaintiff Crystal Hernandez's Experience

65. Plaintiff Crystal Hernandez obtained services from AA of California prior to the Data Breach and received AA of California's *Notice of Data Breach*, dated August 16, 2023, on or about that date. Plaintiff Crystal Hernandez's notice stated that her name and Social Security number were impacted.

66. As a result of the Data Breach, Plaintiff Crystal Hernandez's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Crystal Hernandez's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Crystal Hernandez will have to worry about when and how her sensitive information may be shared or used to her detriment.

67. As a result of the Data Breach notice, Plaintiff Crystal Hernandez spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

68. Additionally, Plaintiff Crystal Hernandez is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

69. Plaintiff Crystal Hernandez stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

70. Plaintiff Crystal Hernandez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

71. Plaintiff Crystal Hernandez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

72. Plaintiff Crystal Hernandez has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Salvador Flores Hernandez's Experience

73. Plaintiff Salvador Flores Hernandez obtained services from AA of California prior to the Data Breach and received AA of California's *Notice of Data Breach*, dated August 16, 2023, on or about that date. Plaintiff Salvador Flores Hernandez's notice stated that his name and Social Security number were impacted.

74. As a result of the Data Breach, Plaintiff Salvador Flores Hernandez's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Salvador Flores Hernandez's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Salvador Flores Hernandez will have to worry about when and how his sensitive information may be shared or used to his detriment.

75. As a result of the Data Breach notice, Plaintiff Salvador Flores Hernandez spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

76. Additionally, Plaintiff Salvador Flores Hernandez is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet

or any other unsecured source.

77. Plaintiff Salvador Flores Hernandez stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

78. Plaintiff Salvador Flores Hernandez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

79. Plaintiff Salvador Flores Hernandez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

80. Plaintiff Salvador Flores Hernandez has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

81. Plaintiffs bring this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

82. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was accessed and/or acquired in the data incident that is the subject of the Notice of Security Incident that Defendants sent to Plaintiffs and Class Members on or around August 16, 2023 (the "Nationwide Class").

83. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate statewide subclass, defined as

follows:

> All individuals who are residents of California and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and Class Members on or around August 16, 2023 (the "California Subclass") (collectively, with the Nationwide Class, "the Classes").

84. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

85. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

86. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendants reported to the South Carolina Attorney General that 79,763 South Carolina residents were impacted in the Data Breach and reported to the Montana Attorney General that 1,280 Montana residents were impacted in the Data Breach and the Classes are apparently identifiable within Defendants' records.

87. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

88. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

89. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

90. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

91. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary

duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

92. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

93. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

94. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

95. Unless a Class-wide injunction is issued, Defendants may continue in their failure

to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

96. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

97. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

98. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

99. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

100. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

101. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendants' possession was adequately secured and protected.

102. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

103. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Nationwide Class. That special relationship arose because Defendants acquired Plaintiffs' and the Nationwide Class's confidential PII in the course of their business practices.

104. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

105. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

106. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, the necessity for encrypting PII, and the necessity for ensuring Defendants maintained the PII in encrypted form.

107. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendants.

108. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in,

and possibly remains in, Defendants' possession.

109. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

110. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

111. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

112. Defendants have admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

113. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendants' possession or control.

114. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

115. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

116. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

117. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

118. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

119. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

120. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud

and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants failed to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

121. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

122. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants failed to undertake appropriate and adequate measures to protect the PII in their continued possession.

123. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the California Subclass and Against AA of California)

124. Plaintiffs and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

125. AA of California's Privacy Policy states "[t]o protect your personal information

from unauthorized access and use, we use security measures that comply with federal law. These measures include administrative, technical, and physical safeguards."

126. In obtaining services from AA of California, Plaintiffs and the California Subclass provided and entrusted their PII to AA of California.

127. AA of California required Plaintiffs and the California Subclass to provide and entrust their PII as condition of obtaining services from AA of California.

128. As a condition of obtaining services from AA of California, Plaintiffs and the California Subclass provided and entrusted their PII. In so doing, Plaintiffs and the California Subclass entered into implied contracts with AA of California by which AA of California agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the California Subclass if their PII had been compromised or stolen.

129. Plaintiffs and the California Subclass fully performed their obligations under the implied contracts with AA of California.

130. AA of California breached the implied contracts it made with Plaintiffs and the California Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII.

131. As a direct and proximate result of AA of California's above-described breach of implied contract, Plaintiffs and the California Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss

and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

132. As a direct and proximate result of AA of California's above-described breach of implied contract, Plaintiffs and the California Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT,
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiffs and the California Subclass and Against AA of California)

133. Plaintiffs and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

134. AA of California violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiffs' and the California Subclass's PII from unauthorized access and exfiltration, theft, or disclosure as a result of AA of California's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

135. The PII of Plaintiffs and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of AA of California's violations of its duty under the CCPA.

136. Plaintiffs and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII,

nominal damages, and additional losses as a direct and proximate result of AA of California's acts described above.

137. AA of California knew, or should have known, that its network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. AA of California failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiffs and members of the California Subclass was exposed.

138. AA of California is organized for the profit or financial benefit of its owners and collects PII as defined in Cal. Civ. Code § 1798.140.

139. AA of California has a gross annual revenue of over $25 million and buys, receives, or sells the personal information of 50,000 or more California residents, households, or devices.

140. Plaintiffs and California Subclass members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5).

141. Pursuant to Section 1798.150(b) of the CCPA, Plaintiffs gave written notice to AA of California of its violations of section 1798.150(a) by certified mail sent on or before August 24, 2023.

142. If within 30 days of Plaintiffs' written notice to AA of California it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written

statement that the violations have been cured and that no further violations shall occur," Plaintiffs will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. See Cal. Civ. Code § 1798.150(b).

COUNT IV
VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiffs and the California Subclass and Against AA of California)

143. Plaintiffs and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

144. The UCL prohibits any "unlawful" or "unfair" business act or practice, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, AA of California engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

145. In the course of conducting its business, AA of California committed "unlawful" business practices by, inter alia, failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and California Subclass members' PII, and by violating the statutory and common law alleged herein, including, inter alia, the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, et seq.), Article I, Section 1 of the California Constitution (California's constitutional right to privacy), Cal. Civil Code § 1798.81.5, 45 C.F.R. § 164, et seq., and Section 5 of the FTC Act. Plaintiffs and California Subclass members reserve the right to allege other violations of law by AA of

California constituting other unlawful business acts or practices. AA of California's above-described wrongful actions, inaction, and want of ordinary care are ongoing and continue to this date.

146. AA of California also violated the UCL by failing to timely notify Plaintiffs and California Subclass members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their Private Information. If Plaintiffs and California Subclass members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their Private Information and identities.

147. AA of California violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein and storing Plaintiffs' and California Subclass members' PII in an unsecure, internet accessible, electronic environment. Specific failures to follow industry standards and exercise reasonable care include: failing to encrypt the PII accessed during the Data Breach; maintaining customer PII for longer than it has a legitimate use; failing to regularly update passwords; failure to implement two-factor authentication for access to accounts and systems containing PII; failing to adequately train employees to recognize phishing and other social engineering techniques; and failing to implement and use software that can adequately detect phishing emails. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass members. The harm these practices caused to Plaintiffs and California Subclass members outweighed their utility, if any.

148. AA of California's above-described wrongful actions, inaction, want of ordinary care, and practices also constitute "unfair" business acts and practices in violation of the UCL in that AA of California's wrongful conduct is substantially injurious to consumers, offends

legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. AA of California's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA and the FTC Act (15 U.S.C. § 45). The gravity of AA of California's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further AA of California's legitimate business interests other than engaging in the above-described wrongful conduct.

149. AA of California engaged in unfair business practices under the "balancing test." The harm caused by AA of California's failure to implement proper data security measures, as described in detail above, greatly outweighs any perceived utility. Indeed, AA of California's failure to follow basic data security protocols cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and California Subclass members, directly causing the harms alleged.

150. AA of California engaged in unfair business practices under the "tethering test." AA of California's failure to implement proper data security measures, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy

Protection Act] is a matter of statewide concern."). AA of California's acts and omissions thus amount to a violation of the law.

151. AA of California engaged in unfair business practices under the "FTC test." The harm caused by AA of California's failure to implement proper data security measures, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. This harm continues given the fact that Plaintiffs' and California Subclass members' PII remains in AA of California's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. AA of California's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, In re LabMD, Inc., FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

152. Plaintiffs and California Subclass members suffered injury in fact and lost money or property as a result of AA of California's violations of statutory and common law. Plaintiffs and the California Subclass suffered from overpaying for services that should have included adequate data security for their PII, by experiencing a diminution of value in their Private Information as a result if its theft by cybercriminals, the loss of Plaintiffs' and California Subclass members' legally protected interest in the confidentiality and privacy of their PII, and additional losses as described above.

153. Plaintiffs and California Subclass members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII for which there is a well-established national and international market (as described above), and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

154. Unless restrained and enjoined, AA of California will continue to engage in the above-described wrongful conduct and more data breaches will occur. As such, Plaintiffs, on behalf of themselves and California Subclass members, seeks restitution and an injunction, including public injunctive relief prohibiting AA of California from continuing such wrongful conduct, and requiring AA of California to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203. To the extent any of these remedies are equitable, Plaintiffs and the Class seek them in the alternative to any adequate remedy at law they may have.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

155. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 95.

156. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

157. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

158. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiffs' and the Nationwide Class's PII, including Social Security numbers and (ii) Defendants' failure to ensure that they stored the PII in encrypted form.

159. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII of Plaintiffs and the Nationwide Class;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiffs harm.

160. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

a. audit, test, and train their data security personnel regarding any new or modified procedures and;

b. implement an education and training program for appropriate employees regarding cybersecurity.

161. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach on Defendants' network. The risk of another such breach is real, immediate, and substantial. If another such breach occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

162. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

163. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Subclass and appointing Plaintiffs and their Counsel to represent such Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

vi. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

vii. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: August 24, 2023

Respectfully Submitted,

/s/ Dylan A. Bess
DYLAN A. BESS, ESQ. (SC BAR NO. 101648)
MORGAN & MORGAN, ATLANTA PLLC
P.O. Box 57007
Atlanta, GA 30343-1007
(404) 965-1886
sbrown@forthepeople.com

Patrick A. Barthle*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
pbarthle@ForThePeople.com

Ryan D. Maxey*
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
(813) 448-1125
ryan@maxeyfirm.com

Jason M. Wucetich*
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Highway, Ste. 2000
El Segundo, California 90245
(310) 335-2001
Jason@wukolaw.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice applications pending*